

CLAIMS:

1. A method for securely generating reports for transmission over a configurable network, the method comprising the steps of:

storing data for a user on a secure data repository and operative in a first processing space inaccessible to the user;

accessing data from the repository to create a secure data file in the first processing space;

providing the secure data file to a second processing space separated from the first processing space by a security device; and

generating the report in the second processing space based upon the secure data file for transmission to the user via the configurable network.

2. The method of claim 1, further comprising generating a report template defining report data for presentation in the report, the secure data file being generated based upon the report data.

3. The method of claim 2, further comprising storing the report template in the second processing space.

4. The method of claim 3, wherein the report is generated in the second processing space based upon the report template and the secure data file.

5. The method of claim 1, further comprising formatting the report in the second processing space for transmission to the user via the configurable network.

6. The method of claim 5, wherein the report is formatted as at least one user viewable page in a markup language.

7. The method of claim 5, wherein the configurable network includes the Internet.

8. The method of claim 1, wherein the second processing space is separated from the configurable network by a second security device.

5 9. The method of claim 1, wherein the data is accessed in accordance with a predetermined reporting schedule.

10 10. The method of claim 1, wherein the data is accessed in response to a user prompt for report generation.

11. The method of claim 1, wherein the security device includes a firewall.

15 12. The method of claim 1, further comprising automatically generating a notification message indicative of availability of the report, and transmitting the notification message to the user via the configurable network.

20 13. The method of claim 12, wherein the report is maintained in the second processing space at least until the user accesses the report via the configurable network.

14. A method for securely generating reports of data associated with a user, the method comprising the steps of:

storing user data associated with the user in a first data repository;

25 transmitting at least a portion of the user data from the first data repository to a second data repository operative in a first processing space inaccessible to the user;

defining a report template, the report template identifying data for presentation in a report;

30 generating a secure data file in the first processing space comprising data identified in the report template;

exporting the secure data file to a second processing space separated from the first processing space and accessible to the user; and

generating the report in the second processing space based upon the template and the data file.

5

15. The method of claim 14, wherein the user data is stored in the first data repository and is synchronized with data stored in the second data repository.

16. The method of claim 14, wherein the first processing space is separated from the second processing space by a firewall.

10

17. The method of claim 14, wherein the user data is transmitted from the first data repository to the second data repository during an automated data collection sequence.

15

18. The method of claim 14, wherein the secure data file is generated in accordance with a predetermined report generation schedule.

19. The method of claim 14, wherein the report is stored in the second processing space at least until accessed by the user.

20

20. A system for generating reports of user data, the system comprising:
a secure data repository operative in a first processing space for storing user data input via a configurable network, the first processing space being inaccessible by the user via the network;

25

a data access program module, operative in the first processing space for extracting report data from the secure data repository;

a second data repository operative in a second processing space securely separated from the first processing space for storing the report data extracted by the data access program module;

30

a report template stored in the second processing space; and

a report generation program module, operative in the second processing space for generating a report based upon the report data and the report template.

5 21. The system of claim 20, wherein the data access program module is configured to extract the desired data in accordance with a predetermined schedule.

 22. The system of claim 20, wherein the second data repository is configured to store the report.

10 23. The system of claim 20, wherein the second data repository is accessible by the user via the network.

 24. The system of claim 20, comprising a server coupled to the second data repository for transmitting the report to the user.

15 25. The system of claim 24, wherein the server is configured to be coupled to a wide area network, and to transmit the report to the medical diagnostic facility via the wide area network.

20 26. The system of claim 20, wherein the first and second processing spaces are separated by a firewall.

 27. A system for securely generating reports for transmission over a configurable network, the system comprising:

25 means for storing data for a user on a secure data repository and operative in a first processing space inaccessible to the user;

 means for accessing data from the repository to create a secure data file in the first processing space;

30 means for providing the secure data file to a second processing space separated from the first processing space by a security device; and

[illegible]